The following is my input to the initial draft of a background document for the Smart Grid part of the *IEEE-USA National Energy Policy Recommendations* document posted at http://www.ieeeusa.org/policy/positions/energypolicy.pdf

This material is my own opinion. It has not been reviewed or approved by IEEE-USA. All, part, or none of this may be included, with or without modification and editing, in an IEEE-USA background document in preparation. This is my first complete draft of my input and has been submitted to the initial part of the process of preparing the document. Whatever part of this winds up in the final document will have to be processed first by a task group, then by the full IEEE-USA Energy Policy Committee, and then by the IEEE-USA Board.

Stan Klein 3-6-2009

An electric power system has two infrastructures:

* An electric infrastructure – that carries the electric energy in the power system, and

* An information infrastructure that monitors, controls, and performs other functions related to the electric infrastructure.

Title XIII of EISA 2007 mandates a "Smart Grid" that is focused on modernizing and improving the information infrastructure.

Some of the technologies relevant to the Smart Grid were initially developed at the Electric Power Research Institute (EPRI) beginning in the late 1980's. EPRI is not a standards developing organization (SDO), so the technology was provided to SDOs for formal standardization. That standards process is ongoing. Initial versions of some standards have been adopted, and it is likely that those standards will be included in the Smart Grid. Relevant technology and standards are also being developed in other venues. It is also likely that there will be gaps, and that additional standards will need to be developed.

The following explanatory material is organized around the specific recommendations contained in the IEEE National Energy Policy Recommendations related to the Smart Grid.

Funding

The Smart Grid efforts have been supported up to now on a voluntary basis. This approach can only proceed slowly, because voluntary efforts compete with funded efforts assigned to participants and are accordingly placed at lower priority. To accomplish the mandated Smart Grid development on a timely basis will require that the funding support authorized in EISA 2007 be provided. Such funding appears to have been provided in the American Recovery and Reinvestment Act.

Need for reference implementations

Many, if not most, traditional standards involve technologies that are well-understood but need some common agreements to make them more easily usable. Examples include dimensions of parts that need to fit together, measurement procedures, and category groupings of test conditions for equipment operating environments (such as temperature and humidity). However, standards related to information

technology often represent new systems designs and require research and development to demonstrate that proposed standards are feasible, unambiguous, and interoperable. A major example is the collection of standards for the Internet, developed by the Internet Engineering Task Force (IETF).

One means of focusing the required R&D is development of one or more reference implementations. A reference implementation creates a definitive interpretation of the draft standard. Before the IETF will adopt a standard, it requires that interoperability be demonstrated between two reference implementations built from different code bases. Only those parts of the draft standard that prove to be interoperable can be included in the adopted standard. The reference implementations are usually openly available, allowing them to be studied by prospective implementers of the standard. The reference implementations also provide the “gold standard” for conformance testing of other implementations.

SDO's that address electric power have processes more focused on traditional standards and do not require development of reference implementations. This leads to adoption of standards that contain errors, ambiguities, and inconsistencies that can best be discovered during attempts at implementation. The usual practice has been to create forums in which these issues can be raised by implementers and resolved in amendments or new editions of the standards.

This situation can be mitigated by developing reference implementations in parallel with development of the standards. For standards that have already been adopted, reference implementations should be developed as soon as possible following adoption, and the identified technical issues fed back rapidly into the standards process.

SDO practices

Unlike the Internet and many other standards that are openly developed and freely downloadable, major SDO's addressing electric power have business models under which they support central staffs by sale of the published standards. Because the standards are developed by committees of volunteers, this creates the need to impose peculiar constraints on the flow of information within the committees and between the committees and outside experts who may have useful suggestions and comments to offer. This requires less openness and limited distribution of content during development.

The requirement for purchasing the standards also creates a barrier to review of the information by potential participant or user personnel who have not been funded to purchase them. This case especially applies to potential organizational "champions" of using or contributing to a standard who are informally attempting to learn the details of the standard prior to making a formal request for organizational funding. It also applies to small businesses and academic projects for which the costs of copies might have significant impact on their available funds.

The information flow constraints created to enforce SDO business models often also create barriers to speed and efficiency in the standards development processes. Flow within the development team and between the development team and outside experts is usually limited to those having a determined "need-to-know" the information in the relevant documents and materials. Such determinations are sometimes error-prone, arbitrary, and counter-productive, especially for materials relevant to information technology standards. To mitigate this, participants sometimes take ad hoc steps that might not agree with the strictest interpretations among SDO management and legal staff.

In addition to the above, there is the consideration that Smart Grid standards are effectively becoming part of US law and regulation. There are court cases suggesting that, in certain situations, when a standard becomes part of law or regulation, the public is entitled to free access. The exact boundaries are unclear and the cases present a difficult judicial issue, but this factor could arise in the context of the Smart Grid.

Some steps that might mitigate this issue include:

- Establishing agreements with SDOs that loosen constraints on standards relevant to the Smart Grid
- Offering funding to the SDOs to replace the US or North American sales for standards relevant to the Smart Grid, thereby allowing the information to be freely distributed both during development and after adoption. Such distribution might be limited to entities that have registered and agreed not to further distribute internationally.
- Otherwise inducing the SDOs to reconsider their business models.

Ratepayer involvement issues

In various venues, regulators and legislators have made it clear that they expect the Smart Grid to result in cost reductions to ratepayers. The justification is that the Smart Grid is intended to improve efficiency, that it should result in cost savings, that the Smart Grid implementation will have to be funded by ratepayers, and the savings should result in payback to the ratepayers through reduced costs. One state regulator even suggested that providers of Smart Grid hardware and software contractually guarantee the savings to ratepayers.

Benefits of the Smart Grid go beyond energy efficiency:

- The Smart Grid will enable use of alternative generation that supports energy independence. Countries that supply energy have often used their positions in the energy markets to advance their national interests unrelated to energy. In addition, many energy supplying countries have interests that are inimical to those of the US. Energy independence mitigates the threat of US policies becoming captive to the interests of energy-supplying countries.
- Components of the Smart Grid will need to have strengthened cyber-security. This helps prevent the well-being of both individual ratepayers and the US economy generally from being harmfully impacted by cyber-attack on Smart Grid facilities. Examples of potential attackers include hostile foreign governments, organized crime, terrorists, market manipulators, and disgruntled employees.
- There are likely to be numerous benefits of the Smart Grid that defy quantification. Examples include the flexibility to accommodate new requirements, the ability to accommodate innovative grid technology, and the ability to support innovative regulatory concepts, all without major replacement of existing equipment.

The flexibility will result in future rate increase avoidance as new technology or requirements arise, but the exact benefit might not be quantifiable until the situation arises in the future. Energy independence and cyber-security are national security issues. This raises the issue of equity between ratepayers and the general public in funding solutions that benefit national security. The relevant regulatory bodies need to recognize and address this issue.

Technologically and economically challenged residential customers

Under some Smart Grid concepts, full participation by residential customers could require them to acquire and use relatively sophisticated devices. Examples of such devices are thermostats and appliances that receive prices from the grid and decide whether to operate based on policies and decision criteria entered by the customer. This raises two issues: economically challenged customers who can not afford the devices, and technologically challenged customers who have difficulty in using the devices.

Addressing these issues will require R&D to minimize the costs of the sophisticated devices and to develop design principles and Smart Grid concepts that best match the capabilities of customers. The latter R&D should consider the knowledge base of Usability Engineering and extensively test the principles and concepts with users of all capabilities.

Coordination with advanced broadband

Many functions in the existing electric grid information infrastructure use legacy protocols and operate over low speed serial lines (e.g., 1200 to 2400 bits per second). Technology that is optimized for low speed serial lines does not have the capability to support the kinds of functions needed in a Smart Grid. Standards that are recognized candidates for the Smart Grid and provide the kinds of needed functionality tend to require higher bandwidths than the legacy technologies.

In addition to funding the Smart Grid, the American Recovery and Reinvestment Act also funds deployment of advanced broadband, with speeds in megabits to gigabits per second. The vision is to make advanced broadband ubiquitous. Such advanced broadband can provide the bandwidth to enable deployment of protocols that provide the advanced functionality needed in the Smart Grid.

Cybersecurity

The Smart Grid will significantly expand the scope, functionality, and capability of the information infrastructure. The downside to this advance is the risk of malicious cyberattack.

Cybersecurity in electric power systems is receiving increased attention. The Department of Homeland Security (DHS), and the Department of Energy (DOE) established a *Roadmap to Secure Control Systems in the Energy Sector*. The North American Electric Reliability Corporation (NERC) adopted Critical Infrastructure Protection (CIP) standards enforceable under the 2005 Energy Policy Act.

EISA 2007 mandates cybersecurity in the Smart Grid. One issue is that Federal jurisdiction extends only to transmission. The NERC CIP standards and the Roadmap tend to focus on issues under Federal jurisdiction. The distribution system, metering, and several other areas addressed in the Smart Grid are under state jurisdiction. Many concepts in the NERC CIP standards and the Roadmap can be used in the state jurisdictional parts of the Smart Grid, but they are likely to require further tailoring and adaptation.

Within the standards community there are efforts underway to address security aspects of the standards they are developing. However, just as the functional standards require testing to demonstrate they are feasible, unambiguous, and interoperable, the security standards require testing. Such testing should

not only ensure that the security standards are feasible, unambiguous, and without adverse impact on interoperability, but that they provide the necessary level of security protection. In addition, any standards developed to fill gaps must have their security addressed.

This will require both attention and resources.